Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions

Benoît Libert\textsuperscript{1,2}  San Ling\textsuperscript{3}  \textbf{Fabrice Mouhartem}\textsuperscript{1}
Khoa Nguyen\textsuperscript{3}  Huaxiong Wang\textsuperscript{3}

\textsuperscript{1}É.N.S. de Lyon, France
\textsuperscript{2}CNRS, France
\textsuperscript{3}Nanyang Technological University, Singapore

Asiacrypt, Hanoi, 06/12/2016
Privacy-Preserving Cryptography

**Important Goal:** Anonymous authentication.
Privacy-Preserving Cryptography

**Important Goal:** Anonymous authentication.

e.g. e-voting, e-cash, group signatures, anonymous credentials...
Privacy-Preserving Cryptography

**Important Goal:** Anonymous authentication.

e.g. e-voting, e-cash, group signatures, anonymous credentials...

**Ingredients**

- A signature scheme
- Zero-knowledge (ZK) proofs
Privacy-Preserving Cryptography

**Important Goal:** Anonymous authentication.

e.g. e-voting, e-cash, group signatures, anonymous credentials...

Ingredients

- A signature scheme
- Zero-knowledge (ZK) proofs compatible with this signature (no hash functions)
Privacy-Preserving Cryptography

**Important Goal:** Anonymous authentication.

e.g. e-voting, e-cash, *group signatures*, anonymous credentials...

**Ingredients**
- A signature scheme
- Zero-knowledge (ZK) proofs compatible with this signature (no hash functions)
Group Signatures

A user wants to take public transportations.
Group Signatures

A user wants to take public transportations.

timestamp

[Image of a user and a timestamp]
Group Signatures

A user wants to take public transportations.

- Authenticity & Integrity
A user wants to take public transportations.

- Authenticity & Integrity
- Anonymity
A user wants to take public transportations.

- **Authenticity & Integrity**
- **Anonymity**
- **Dynamicity**
A user wants to take public transportations.

- Authenticity & Integrity
- Anonymity
- Dynamicity
- Traceability
Motivation

**Dynamic group signatures**

In *dynamic* group signatures, new group members can be introduced *at any time*.

The *dynamic* group setting:
Motivation

**Dynamic group signatures**

In **dynamic** group signatures, new group members can be introduced **at any time**.

The **dynamic** group setting:

- Add users without re-running the **Setup** phase;
Motivation

**Dynamic group signatures**

In **dynamic** group signatures, new group members can be introduced at any time.

The **dynamic** group setting:

- Add users without re-running the **Setup** phase;
- Even if everyone, including authorities, is dishonest, no one can sign in your name;
Motivation

**Dynamic** group signatures

In **dynamic** group signatures, new group members can be introduced *at any time*.

The **dynamic** group setting:

- Add users without re-running the **Setup** phase;
- Even if everyone, including authorities, is dishonest, no one can sign in your name;
- Most use cases require dynamic groups (e.g., anonymous access control in buildings).
## Anonymous Credentials (Chaum'85, Camenisch-Lysyanskya'01)

### Principle (e.g., U-Prove, Idemix)

Involves **Authority, Users and Verifiers**.

- User dynamically obtains credentials from an authority under a pseudonym (= commitment to a digital identity)
- ... and can dynamically prove possession of credentials using different (*unlinkable*) pseudonyms

### Different flavors: one-show/multi-show credentials, attribute-based access control, ...
Anonymous Credentials (Chaum'85, Camenisch-Lysyanskya’01)

**Principle** (e.g., U-Prove, Idemix)

Involves **Authority, Users and Verifiers**.

- User dynamically obtains credentials from an authority under a pseudonym (= commitment to a digital identity)
- ...and can dynamically prove possession of credentials using different (*unlinkable*) pseudonyms

**Different flavors**: one-show/multi-show credentials, attribute-based access control,...

**General construction** from signature with efficient protocols:

- Authority gives a user a signature on a committed message;
- User proves that same secret underlies different pseudonyms;
- User proves that he possesses a message-signature pair.
Signature with Efficient Protocols

Signature Scheme with Efficient Protocols
(Camenisch-Lysyanskya, SCN’02)

Signer

Verifier

Message

Signature

Message

Sign

Verify
Signature with Efficient Protocols

Signature Scheme with Efficient Protocols
(Camenisch-Lysyanskya, SCN’02)

- Protocol for signing committed messages
Signature with Efficient Protocols

Signature Scheme with Efficient Protocols
(Camenisch-Lysyanskya, SCN’02)

- Protocol for signing committed messages
- Proof of Knowledge (PoK) of (Message; Signature)
A lattice is a discrete subgroup of $\mathbb{R}^n$. Can be seen as integer linear combinations of a finite set of vectors.

$$\Lambda(b_1, \ldots, b_n) = \left\{ \sum_{i \leq n} a_i b_i \mid a_i \in \mathbb{Z} \right\}$$
Lattice-Based Cryptography

Lattice

A lattice is a discrete subgroup of $\mathbb{R}^n$. Can be seen as integer linear combinations of a finite set of vectors.

$$\Lambda(b_1, \ldots, b_n) = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in \mathbb{Z} \right\}$$

Why?

- Simple and efficient;
- Still conjectured quantum-resistant;
- Connection between average-case and worst-case problems;
- Powerful functionalities (e.g., FHE).

→ Finding a non-zero short vector in a lattice is hard.
Hardness Assumptions: SIS and LWE

**Parameters:** \( n \) dimension, \( m \geq n \), \( q \) modulus.

For \( A \leftarrow \mathcal{U}(\mathbb{Z}_q^{m \times n}) \):

<table>
<thead>
<tr>
<th>Small Integer Solution</th>
<th>Learning With Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x ) ( \mathbb{Z}^m {0} ) small</td>
<td>( s \leftarrow \mathbb{Z}_q^n ) small error</td>
</tr>
</tbody>
</table>

Goal: Given \( A \in \mathbb{Z}_q^{m \times n} \), find \( x \in \mathbb{Z}^m \{0\} \) small

Goal: Given \( (A, As + e) \), find \( s \in \mathbb{Z}_q^n \)
Group Signatures: History

1991 Chaum and van Heyst: introduction

2000 Ateniese, Camenisch, Joye and Tsudik: first scalable solution

2003 Bellare, Micciancio and Warinschi: model for static groups
Group Signatures: History

1991 Chaum and van Heyst: introduction

2000 Ateniese, Camenisch, Joye and Tsudik: first scalable solution

2003 Bellare, Micciancio and Warinschi: model for static groups

2004 Kiayias and Yung: model for dynamic groups

2004 Bellare, Shi and Zhang: model for dynamic groups
Group Signatures: History

1991 Chaum and van Heyst: introduction
2000 Ateniese, Camenisch, Joye and Tsudik: first scalable solution
2003 Bellare, Micciancio and Warinschi: model for static groups
2004 Kiayias and Yung: model for dynamic groups
2004 Bellare, Shi and Zhang: model for dynamic groups
2010 Gordon, Katz and Vaikuntanathan: first lattice-based scheme
2013 Laguillaumie, Langlois, Libert and Stehlé: log-size signatures from lattices
Group Signatures: History

1991 Chaum and van Heyst: introduction

2000 Ateniese, Camenisch, Joye and Tsudik: first scalable solution

2003 Bellare, Micciancio and Warinschi: model for static groups

2004 Kiayias and Yung: model for dynamic groups

2004 Bellare, Shi and Zhang: model for dynamic groups

2010 Gordon, Katz and Vaikuntanathan: first lattice-based scheme

2013 Laguillaumie, Langlois, Libert and Stehlé: log-size signatures from lattices

No dynamic group signature scheme based on lattices
Outline

Introduction

Anonymous Credentials and Group Signatures
  Motivations
  Intuition

Our Constructions

Conclusion
Signature with Efficient Protocols (CL'02)

A signature scheme \((\text{Keygen, Sign}_{sk}, \text{Verif}_{vk})\) with protocols:

- Sign a committed value;
- Prove possession of a signature.
Signature with Efficient Protocols (CL’02)

A signature scheme \((\text{Keygen}, \text{Sign}_{sk}, \text{Verif}_{vk})\) with protocols:
- Sign a committed value;
- Prove possession of a signature.

Security
- Unforgeability;
- Security of the two protocols;
- Anonymity.

→ many applications for privacy-based protocols.
Signature with Efficient Protocols (CL'02)

A signature scheme \((\text{Keygen}, \text{Sign}_{sk}, \text{Verif}_{vk})\) with protocols:
- Sign a committed value;
- Prove possession of a signature.

Security
- Unforgeability;
- Security of the two protocols;
- Anonymity.

→ many applications for privacy-based protocols.

*Existing constructions rely on Strong RSA assumption or bilinear maps.*
**Dynamic Group Signature**

It is a tuple of algorithms *(Setup, Join, Sign, Verify, Open)* acting according to their names.
Dynamic Group Signature

It is a tuple of algorithms (Setup, Join, Sign, Verify, Open) acting according to their names.

- **Setup:**
  - **Input:** security parameter $\lambda$, bound on group size $N$
  - **Output:** public parameters $Y$, group manager’s secret key $S_{GM}$, the opening authority’s secret key $S_{OA}$;
Dynamic Group Signature

It is a tuple of algorithms (Setup, Join, Sign, Verify, Open) acting according to their names.

- **Join**: interactive protocols between \( U_i \leftrightarrow GM \). Provide \((\text{cert}_i, \text{sec}_i)\) to \( U_i \). Where \( \text{cert}_i \) attests the secret \( \text{sec}_i \). Update the user list along with the certificates;
Dynamic Group Signature

It is a tuple of algorithms \((\text{Setup}, \text{Join}, \text{Sign}, \text{Verify}, \text{Open})\) acting according to their names.

- **Sign** and **Verify** proceed in the obvious way;
- **Open**:
  - Input: OA’s secret \(S_{OA}\), \(M\) and \(\Sigma\)
  - Output: \(i\).
Three security notions

- **Anonymity**: only OA can open a signature;
Security

Three security notions

- **Anonymity**: only OA can open a signature;

- **Traceability** (≡ security of honest GM against users): no coalition of malicious users can create a signature that cannot be traced to one of them;
Security

Three security notions

- **Anonymity**: only OA can open a signature;

- **Traceability** (= security of honest GM against users): no coalition of malicious users can create a signature that cannot be traced to one of them;

- **Non-frameability** (= security of honest members): colluding GM and OA cannot frame honest users.
Outline

Introduction

Anonymous Credentials and Group Signatures
Motivations
Intuition

Our Constructions

Conclusion
Signature with Efficient Protocols

Based on a variant of Boyen’s signature (PKC’10)

Given \( \mathbf{A} \in \mathbb{Z}_{q}^{n \times m} \) and \( \{ \mathbf{A}_i \}_{i=0}^{\ell} \in \mathbb{Z}_{q}^{n \times m} \), the signature is a small \( \mathbf{d} \in \mathbb{Z}^{2m} \) s.t.

\[
\mathbf{A} \mathbf{A}_0 + \sum_{j=1}^{\ell} m_j \mathbf{A}_j \cdot \mathbf{d} = 0 \ [q].
\]

The private key is a short \( \mathbf{T}_\mathbf{A} \in \mathbb{Z}^{m \times m} \) s.t.

\[
\mathbf{A} \cdot \mathbf{T}_\mathbf{A} = 0 \ [q].
\]
Signature with Efficient Protocols

Based on a variant of Boyen’s signature (PKC’10)

Given \( A \in \mathbb{Z}_{q}^{n \times m} \) and \( \{A_{i}\}_{i=0}^{\ell} \in \mathbb{Z}_{q}^{n \times m} \), the signature is a small

\[
d \in \mathbb{Z}^{2m} \text{ s.t. } A \left( A_{0} + \sum_{j=1}^{\ell} m_{j} A_{j} \right) \cdot d = 0 \ [q].
\]

The private key is a short \( T_{A} \in \mathbb{Z}^{m \times m} \) s.t. \( A \cdot T_{A} = 0 \ [q] \).

(A modification of) Böhl et al.’s variant (Eurocrypt’13)

\( \tau \leftarrow \mathcal{U}(\{0,1\}^{\ell}) \), \( D \) and \( u \) are public, \( m \in \{0,1\}^{2m} \) encodes Msg.

\[
A \left( A_{0} + \sum_{j=1}^{\ell} \tau_{j} A_{j} \right) \cdot d = u + D \cdot m \ [q].
\]

\( \rightarrow \quad \sigma = (\tau, d) \)
Our Signature with Efficient Protocols

To sign $M \in \{0, 1\}^{2m}$:

- Sample random $\tau \in \{0, 1\}^\ell$
Our Signature with Efficient Protocols

To sign $M \in \{0, 1\}^{2m}$:

- Sample random $\tau \in \{0, 1\}^\ell$, random $s \in D\mathbb{Z}^{2m, \tilde{\sigma}}$
- Compute $C_M = D_0 \cdot s + D_1 \cdot M \in \mathbb{Z}_q^{2n}$
Our Signature with Efficient Protocols

To sign $M \in \{0, 1\}^{2m}$:

- Sample random $\tau \in \{0, 1\}^\ell$, random $s \in D_{\mathbb{Z}^{2m}, \tilde{\sigma}}$
- Compute $C_M = D_0 \cdot s + D_1 \cdot M \in \mathbb{Z}_q^{2n}$
- Using $T_A$, sample a short $d$ s.t.

\[
A = A_0 + \sum_{j=1}^\ell \tau_j \cdot A_j
\]

\[
u \quad + \quad D \quad = \quad \text{bin}(C_M) \quad (*)
\]

$\Sigma = (\tau, \underline{d}, s) \in \{0, 1\}^\ell \times \mathbb{Z}^{2m} \times \mathbb{Z}^{2m}$

To verify: check that $d$ is short and that $\Sigma$ satisfies $(*)$. 

Fabrice Mouhartem  Signatures with Efficient Protocols and Lattice-Based Dynamic GS  06.12.2016  16/30
Our Signature with Efficient Protocols

Kawachi et al.’s commitment (Asiacrypt’08):

\[ C_M = D_0 \cdot s + D_1 \cdot M \]

Is already embedded in Böhl et al. signature.
Our Signature with Efficient Protocols

Kawachi et al.’s commitment (Asiacrypt'08):

\[ C_M = D_0 \cdot s + D_1 \cdot M \]

Is already embedded in Böhl et al. signature.

**Difficulty:** In the proof, for one of the queries, the signature has a different distribution.
Our Signature with Efficient Protocols

Kawachi et al.’s commitment (Asiacrypt’08):

\[ C_M = D_0 \cdot s + D_1 \cdot M \]

Is already embedded in Böhl et al. signature.

**Difficulty:** In the proof, for one of the queries, the signature has a different distribution.

**Solution:** Use Rényi divergence instead of statistical distance to bound adversary’s advantage [BLLSS15].

\[
R_a(P \| Q) = \left( \sum_{x \in \text{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{1/(a-1)}
\]
Our Signature **with Efficient Protocols**

Kawachi *et al.*’s commitment ([Asiacrypt’08]):

\[ C_M = D_0 \cdot s + D_1 \cdot M \]

Is already embedded in Böhl *et al.* signature.

**Difficulty**: In the proof, for one of the queries, the signature has a different distribution.

**Solution**: Use Rényi divergence instead of statistical distance to bound adversary’s advantage [BLLSS15].

\[
R_a(P \| Q) = \left( \sum_{x \in \text{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{1/(a-1)}
\]

**Probability Preservation**: \( Q(A) \geq P(A)^{\frac{a}{a-1}} / R_a(P \| Q) \)
Our Signature with efficient protocols

Kawachi *et al.* commitment (Asiacrypt’08):

For $D_0, D_1 \in \mathbb{Z}^{2n \times 2m}_q$, $s \leftarrow D_{\mathbb{Z}^{2m}, \sigma}$, $M \in \{0, 1\}^{2m}$

$$C_M = D_0 \cdot s + D_1 \cdot M [q]$$

Compatible with Stern’s protocol (Crypto’93, [LNSW; PKC’13])

$\implies$ ZK proof compatible with the signature
Stern’s Protocol (Crypto’93)

**Stern’s protocol**: a ZK proof for Syndrome Decoding Problem.
Stern’s Protocol (Crypto’93)

**Stern’s protocol:** a ZK proof for Syndrome Decoding Problem.

**Syndrome Decoding Problem**

| P ∈ \(\mathbb{Z}_2^{n \times m}\) and \(v ∈ \mathbb{Z}_2^n\), find \(x\) s.t. \(w(x) = w\) and \(P \cdot x = v \pmod{2}\) |
Stern’s Protocol (Crypto’93)

**Stern’s protocol**: a ZK proof for Syndrome Decoding Problem.

### Syndrome Decoding Problem

Given \( P \in \mathbb{Z}_2^{n \times m} \) and \( v \in \mathbb{Z}_2^n \), find \( x \) s.t. \( w(x) = w \) and

\[
P \cdot x = v \mod 2
\]

\[\text{mod } 2 \rightarrow \text{mod } q\]

[**KTX08**]: Extend Stern’s protocol for SIS and LWE statements

Recent uses of Stern-like protocols in lattice-based crypto:

[**LNW15, LLNW16, LLNMW16**]
Unified Framework using Stern’s Protocol

**Problem**: protocols using Stern’s proofs build them “from scratch”.  
[LNW15, LLNW16]
Unified Framework using Stern’s Protocol

**Problem**: protocols using Stern’s proofs build them “from scratch”. [LNW15, LLNW16]

Provide a framework to construct ZKAoK:
- to prove knowledge of an $x \in \{-1, 0, 1\}^n$ of a special form verifying $P \cdot x = v \mod q$
  - many lattice statements reduce to this
  - this captures various and complex statements
Unified Framework using Stern’s Protocol

**Problem**: protocols using Stern’s proofs build them “from scratch”. [LNW15, LLNW16]

Provide a framework to construct ZKAoK:

- to prove knowledge of an \( \mathbf{x} \in \{-1, 0, 1\}^n \) of a special form verifying \( \mathbf{P} \cdot \mathbf{x} = \mathbf{v} \mod q \)
  - many lattice statements reduce to this
  - this captures various and complex statements
- that uses [LNSW13]’s decomposition-extension framework and is combinatoric in Stern’s protocol manner
From Static to Dynamic

- Designed from a recent static group signature proposed by Ling, Nguyen and Wang [LNW15];
From Static to Dynamic

- Designed from a recent static group signature proposed by Ling, Nguyen and Wang [LNW15];

- **Non-frameability** requires to introduce **non-homogeneous terms** in the SIS relations satisfied by membership certificates;
From Static to Dynamic

- Designed from a recent static group signature proposed by Ling, Nguyen and Wang [LNW15];

- **Non-frameability** requires to introduce **non-homogeneous terms** in the SIS relations satisfied by membership certificates;

- Other solutions [LLLS13, NZZ15] use membership certificates made of a complete basis...

  ...which is problematic with **non-homogeneous terms** (would give too much freedom to group members).
From Static to Dynamic
Difficulties (1/2)

- Separate the secrets between OA and GM;
From Static to Dynamic
Difficulties (1/2)

- Separate the secrets between OA and GM;

- Bind the user’s secret $z_i$ to a unique public syndrome
  \[ v_i = F \cdot z_i \in \mathbb{Z}_q^{4n} \text{ for some matrix } F \in \mathbb{Z}_q^{4n \times 4m}; \]
From Static to Dynamic

Difficulties (1/2)

- Separate the secrets between OA and GM;

- Bind the user’s secret $z_i$ to a unique public syndrome $v_i = F \cdot z_i \in \mathbb{Z}_q^{4n}$ for some matrix $F \in \mathbb{Z}_q^{4n \times 4m}$;

Use our signature scheme with efficient protocols:

\[
A = A_0 + \sum_{j=1}^{\ell} \text{id}_j \cdot A_j
\]

\[
d = u + D
\]

\[
\text{bin}(C_{v_i})
\]
From Static to Dynamic

Difficulties (2/2)

- **Difficulty**: achieving security against **framing attacks**:
  - i.e., even a dishonest GM cannot create signatures that open to honest users
  - Users need a membership certificate with a membership secret
  - GM must certify that public key
Difficulty: achieving security against framing attacks:

- i.e., even a dishonest GM cannot create signatures that open to honest users
- Users need a membership certificate with a membership secret
- GM must certify that public key

Be secure against framing attacks without compromising previous security properties;
From Static to Dynamic Our solution

Setup:

**Group public key:** \( \mathcal{Y} = (A, \{A_i\}_{i=0}^\ell, B, D, D_0, D_1, F, u) \)

\( \ell = \log(N) \) (e.g. \( \ell = 30 \))
From Static to Dynamic Our solution

Setup:

Group public key: \( \mathcal{Y} = (A, \{A_i\}_{i=0}^{\ell}, B, D, D_0, D_1, F, u) \)

\( \ell = \log(N) \) (e.g. \( \ell = 30 \))

Join algorithm:

\( U_i \) \hspace{6cm} \text{GM}
From Static to Dynamic Our solution

Setup:

Group public key: \( \mathcal{Y} = (A, \{A_i\}_{i=0}^\ell, B, D, D_0, D_1, F, u) \)

\( \ell = \log(N) \) (e.g. \( \ell = 30 \))

Join algorithm:

\[ U_i \]

\[ z_i \leftarrow \text{short vector in } \mathbb{Z}^{4m} \]

\[ v_i = F \cdot z_i \]
From Static to Dynamic Our solution

Setup:

Group public key: \( \mathcal{Y} = (A, \{A_i\}_{i=0}^{\ell}, B, D, D_0, D_1, F, u) \)

\( \ell = \log(N) \) (e.g. \( \ell = 30 \))

Join algorithm:

\( \mathcal{U}_i \)

\( z_i \leftarrow \text{short vector in } \mathbb{Z}^{4m} \)

\( v_i = F \cdot z_i \)

GM

\( v_i \)

\( v_i \)

\( \text{id}_i \leftarrow \text{identity} \in \{0, 1\}^\ell \)

\( \text{cert}_i \triangleq (\text{id}_i, d_i, s_i) = \text{Sign}(v_i) \)
From Static to Dynamic Our solution

Setup:

**Group public key:** \( \mathcal{Y} = (A, \{A_i\}_{i=0}^\ell, B, D, D_0, D_1, F, u) \)

\( \ell = \log(N) \) (e.g. \( \ell = 30 \))

Join algorithm:

\( U_i \)

\( z_i \leftarrow \text{short vector in } \mathbb{Z}^{4m} \)

\( v_i = F \cdot z_i \)

GM

\( v_i \)

id\( _i \leftarrow \text{identity } \in \{0, 1\}^\ell \)

If (id\( _i, d_i, s_i \))

does not verify, abort

\( (sec_i; cert_i) = (z_i, (id_i, d_i, s_i)) \)
From Static to Dynamic Our solution — further steps

<table>
<thead>
<tr>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCA-Anonymity: anonymity in presence of an opening oracle.</td>
</tr>
</tbody>
</table>
From Static to Dynamic Our solution — further steps

Goal

CCA-Anonymity: anonymity in presence of an opening oracle.

Canetti-Halevi-Katz transformation (Eurocrypt’04)

Any IBE implies IND-CCA-secure encryption.

Identity Based Encryption (Shamir’84, Boneh-Franklin’01)

- Encryption computes $C \leftarrow \text{Enc}(MPK, ID, M)$
- Decryption computes $M \leftarrow \text{Dec}(MPK, C, d_{ID})$ where $d_{ID} \leftarrow \text{Keygen}(MSK, ID)$
From Static to Dynamic Our solution

\textbf{Sign} algorithm:
\[
c := \text{Enc}(v_i)
\]
From Static to Dynamic: Our solution

**Sign** algorithm:
\[ c := \text{Enc}(v_i) \quad \pi_K := \text{proof that } c \text{ is correct and that} \]

\[
\begin{align*}
A & \equiv A_0 + \sum_{j=1}^{\ell} \text{id}_j \cdot A_j \\
\equiv d & = u + D \\
\text{bin}(C_{v_i})
\end{align*}
\]

Message is bound to \( \pi_K \) via the hash function of the Fiat-Shamir paradigm (signature of knowledge).
From Static to Dynamic Our solution

**Verify** algorithm:

- A user verifies if $\pi_K$ is correct.
From Static to Dynamic: Our solution

**Verify** algorithm:

- A user verifies if $\pi_K$ is correct.

**Open** algorithm:

- **OA** decrypts $c$ to get $v_i$;
- **OA** searches for the associated $i$ in the Join transcripts, and if so, returns $i$, otherwise abort.
Outline

Introduction

Anonymous Credentials and Group Signatures
   Motivations
   Intuition

Our Constructions

Conclusion
Summary

- Lattice-based signature with efficient protocols;
  - for obtaining signatures on committed message;
  - for proving possession of a message-signature pair.
- First dynamic group signature based on lattice assumptions;
  - use simpler version of our signature with efficient protocols;
  - enables round-optimal, concurrent joins (Kiayias-Yung, EC'05).
- Unified framework for proving modular linear equations using Stern’s technique.

Technical contributions:

- Combine Böhl et al. signatures + Ling et al. ZK proofs $\implies$ signature with efficient protocols;
- A method of signing public keys so that knowledge of the secret key can be efficiently proved (cf. structure-preserving cryptography).
Thank you all for your attention!
## Group Signatures: Comparative Table

<table>
<thead>
<tr>
<th>Scheme</th>
<th>LLLS</th>
<th>NZZ</th>
<th>LNW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group PK</td>
<td>$\tilde{O}(\lambda^2) \cdot \log N_{gs}$</td>
<td>$\tilde{O}(\lambda^2)$</td>
<td>$\tilde{O}(\lambda^2) \cdot \log N_{gs}$</td>
</tr>
<tr>
<td>User’s SK</td>
<td>$\tilde{O}(\lambda^2)$</td>
<td>$\tilde{O}(\lambda^2)$</td>
<td>$\tilde{O}(\lambda)$</td>
</tr>
<tr>
<td>Signature</td>
<td>$\tilde{O}(\lambda) \cdot \log N_{gs}$</td>
<td>$\tilde{O}(\lambda + \log^2 N_{gs})$</td>
<td>$\tilde{O}(\lambda) \cdot \log N_{gs}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scheme</th>
<th>LLNW</th>
<th>Ours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group PK</td>
<td>$\tilde{O}(\lambda^2)$</td>
<td>$\tilde{O}(\lambda^2) \cdot \log N_{gs}$</td>
</tr>
<tr>
<td>User’s SK</td>
<td>$\tilde{O}(\lambda) \cdot \log N_{gs}$</td>
<td>$\tilde{O}(\lambda)$</td>
</tr>
<tr>
<td>Signature</td>
<td>$\tilde{O}(\lambda) \cdot \log N_{gs}$</td>
<td>$\tilde{O}(\lambda) \cdot \log N_{gs}$</td>
</tr>
</tbody>
</table>
Definition

A one-time signature scheme consists of a triple of algorithms \( \Pi^{\text{ots}} = (G, S, V) \). Behaves like a digital signature scheme.

**Strong unforgeability**: impossible to forge a valid signature even for a previously signed message.

Usage

We use one-time signature to provide CCA anonymity using Canetti-Halevi-Katz methodology.
CCA anonymity

Definition

No PPT adversary $\mathcal{A}$ can win the following game with non negligible probability:

1. $\mathcal{A}$ makes open queries.
2. $\mathcal{A}$ chooses $M^*$ and two different $(\text{cert}_i^*, \text{sec}_i^*)_{i \in \{0, 1\}}$.
3. $\mathcal{A}$ receives $\sigma^* = \text{Sign}_{\text{cert}_b^*, \text{sec}_b^*}(M^*)$ for some $b \in \{0, 1\}$.
4. $\mathcal{A}$ makes other open queries.
5. $\mathcal{A}$ returns $b'$, and wins if $b = b'$.
ZK Proofs

<table>
<thead>
<tr>
<th>$\Sigma$-protocol [Dam10]</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-move scheme: <em>(Commit, Challenge, Answer)</em> <em>between 2 users.</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fiat-Shamir Heuristic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make the $\Sigma$-protocol <strong>non-interactive</strong> by setting the challenge to be $H(\text{Commit}, \text{Public})$</td>
</tr>
</tbody>
</table>
From Static to Dynamic  Our solution – Ingredients

Security proof of the Boyen signature

Lattice algorithms use short basis as *trapdoor* information.

**SampleUp**

\[
A' = \begin{bmatrix} A \\ B \cdot A + C \end{bmatrix} \in \mathbb{Z}_q^{2m \times n}, A \in \mathbb{Z}_q^{m \times n}, T_A \in \mathbb{Z}_q^{m \times m}, \sigma \mapsto \text{gaussian } v \in \mathbb{Z}_q^n, \text{ s.t. } v^T A' = 0[q]
\]

**SampleDown**

\[
A' = \begin{bmatrix} A \\ B \cdot A + C \end{bmatrix} \in \mathbb{Z}_q^{2m \times n}, C \in \mathbb{Z}_q^{m \times n}, T_C \in \mathbb{Z}_q^{m \times m}, \sigma \mapsto \text{gaussian } v \in \mathbb{Z}_q^n, \text{ s.t. } v^T A' = 0[q]
\]
From Static to Dynamic  

Our solution – Ingredients

Security proof of the Boyen signature

Boyen’s signature

$$d^T \left[ \frac{A}{A_0 + \sum_{i=1}^{\ell} m_i A_i} \right] = 0[q]$$

Idea. Set $A_i = Q_i A + h_i C$

$$\rightarrow \left[ \frac{A}{A_0 + \sum_{i=1}^{\ell} m_i A_i} \right] = \left[ \frac{A}{(Q_0 + \sum_{i=1}^{\ell} m_i Q_i)A + h_M C} \right]$$

$\Rightarrow$ We can use SampleUp in the real setup and SampleDown in the reduction whenever $h_M \neq 0$. 

From Static to Dynamic Our solution – Ingredients

Security proof of the Boyen signature

Recall

\[ A' := \begin{bmatrix} A \\ A_0 + \sum_{i=1}^{\ell} m_i A_i \end{bmatrix} = \begin{bmatrix} A \\ (Q_0 + \sum_{i=1}^{\ell} m_i Q_i)A + h_M C \end{bmatrix} \]

Forgery. \( A \) outputs \( d^* = [d_1^T \, d_2^T]^T \) and \( M^* = m_1^* \ldots m_\ell^* \) such that \( d^{*T} A' = 0 \).

If \( h_{M^*} = 0 \), then

\[
\left( d_1^* T + d_2^* T \left( Q_0 + \sum_{i=1}^{\ell} m_i^* Q_i \right) \right) A = 0[q]
\]

valid SIS solution
Remark

Boyen’s signature: the reduction aborts if $C$ vanishes.
Böhl et al.: answer the request by “programming” the vector

$$u^T = d^T \left[ \frac{A}{(Q_0 + \sum_{i=1}^{\ell} m_i^T Q_i)A} \right] - z_i^T D.$$

Problem

In this request, a sum of two discrete gaussian is generated differently from the real Join protocol.
⇒ Not the same standard deviation.
From Static to Dynamic  

Our solution

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>$z_i,0, z_i,1, z_i \in \mathbb{Z}^m$</td>
</tr>
</tbody>
</table>

Consequence.

$$\{(z_i, z_i,0, z_i,1)|z_i,0 \leftarrow D_{\sigma_0}, z_i,1 \leftarrow D_{\sigma_1}, z_i = z_i,0 + z_i,1\}$$

\[\Delta\]

$$\{(z_i, z_i,0, z_i,1)|z_i \leftarrow D_{\sigma}, z_i,0 \leftarrow D_{\sigma_0}, z_i,1 = z_i - z_i,0\}$$
Rényi Divergence

\[ R_a(P \parallel Q) = \left( \sum_{x \in \text{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{1/(a-1)} \]
Rényi Divergence

Presentation

\[ R_a(P \parallel Q) = \left( \sum_{x \in \text{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{1/(a-1)} \]

- Measurement of the distance between two distributions
Rényi Divergence

Presentation

\[ R_a(P \parallel Q) = \left( \sum_{x \in \text{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{1/(a-1)} \]

- Measurement of the distance between two distributions
- Multiplicative instead of additive
- Probability preservation:

\[ Q(A) \geq P(A)^{\frac{a}{a-1}} / R_a(P \parallel Q) \]
Rényi Divergence

Hybrid argument:

Real game $\rightarrow$ Game 1 $\rightarrow$ Game 2 $\rightarrow$ Hard Game

- Hardness assumptions -

Bound winning probability.
Can be done through probability preservation!

Recall

\[
Q(A) \geq P(A)\frac{a}{a-1} / R_a(P \parallel Q)
\]

\[
\Pr[W_2] \geq \Pr[W_1]^{\frac{a}{a-1}} / R_a(Game_1 \parallel Game_2)
\]

For instance:

\[
\Pr[W_2] \geq \Pr[W_1]^2 / R_2(Game_1 \parallel Game_2)
\]
Rényi Divergence
In Crypto

Consequence

Usually use *statistical distance* to measure distance between probabilities.

→ In our setting, implies $q \sim \exp(\lambda)$ (*smudging*)

→ Higher cost compared to usual lattice-based crypto parameters